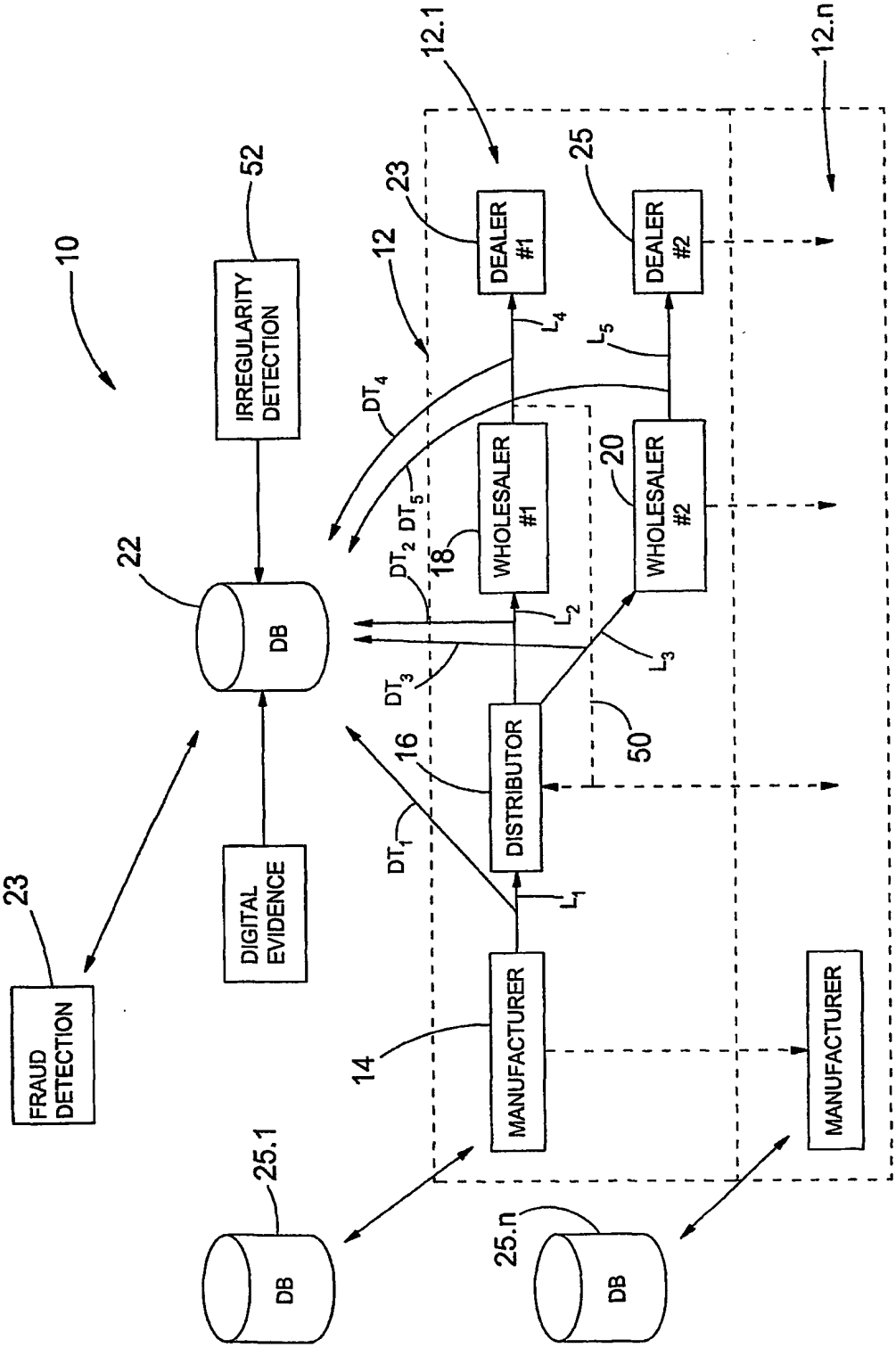
10
IRREGULARITY DETECTION
52
DB
22
DIGITAL EVIDENCE
FRAUD DETECTION
23
DB
25.1
DB
25.n
12
12.1
12.n
DEALER #1
23
DEALER #2
25
WHOLESALER #1
18
WHOLESALER #2
20
DISTRIBUTOR
16
MANUFACTURER
14
MANUFACTURER
50
DT1
DT2
DT3
DT4
DT5
L1
L2
L3
L4
L5

FIGURE 1

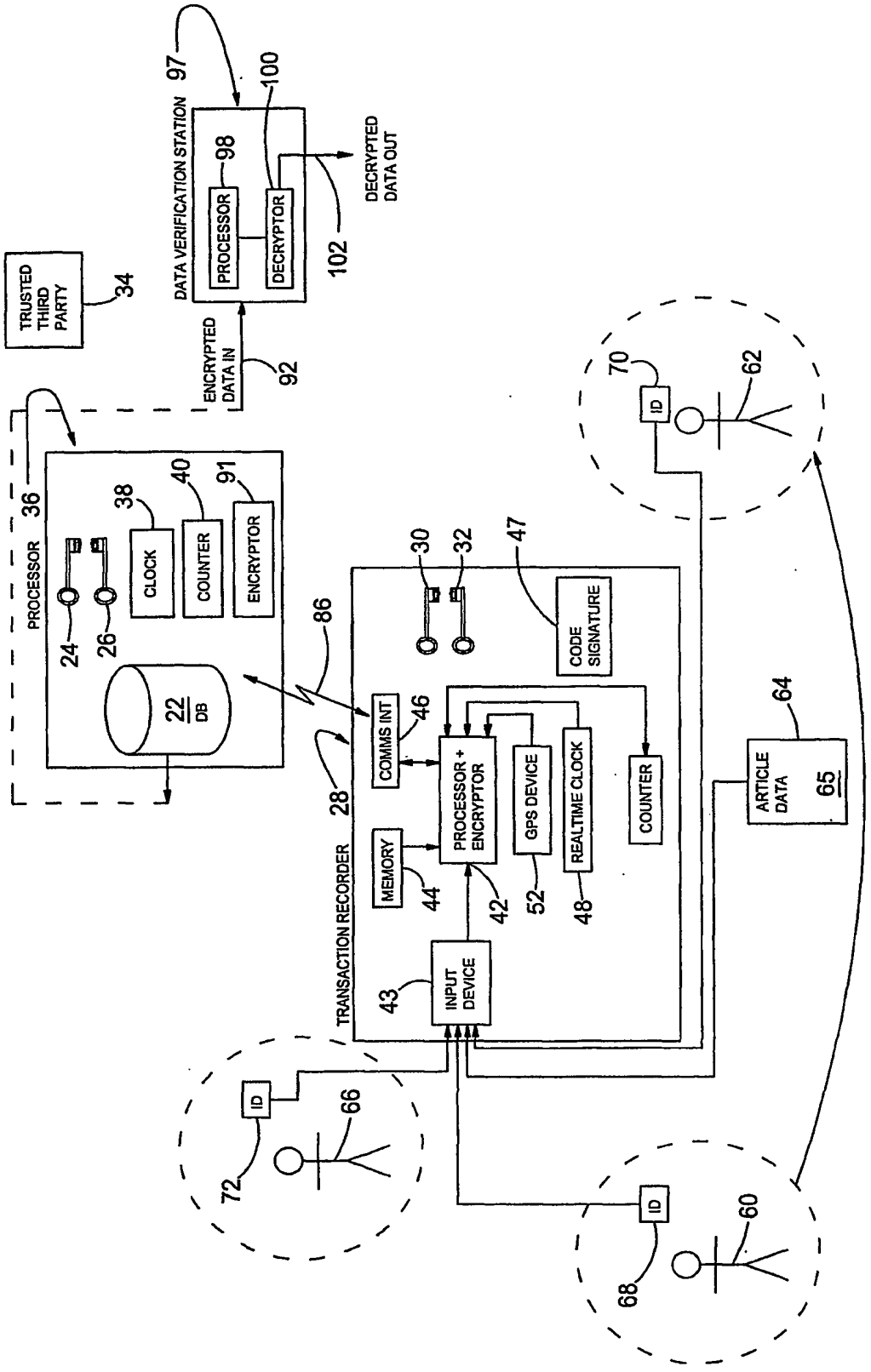
97
100
DATA VERIFICATION STATION
98
PROCESSOR
DECRYPTOR
102
DECRYPTED DATA OUT
TRUSTED THIRD PARTY
34
ENCRYPTED DATA IN
92
36
PROCESSOR
38
CLOCK
40
COUNTER
91
ENCRYPTOR
24
26
22
DB
86
30
32
47
CODE SIGNATURE
COMMS INT
46
28
TRANSACTION RECORDER
MEMORY
44
PROCESSOR + ENCRYPTOR
42
GPS DEVICE
52
REALTIME CLOCK
48
COUNTER
INPUT DEVICE
43
70
ID
62
64
ARTICLE DATA
65
72
ID
66
68
ID
60

FIGURE 2

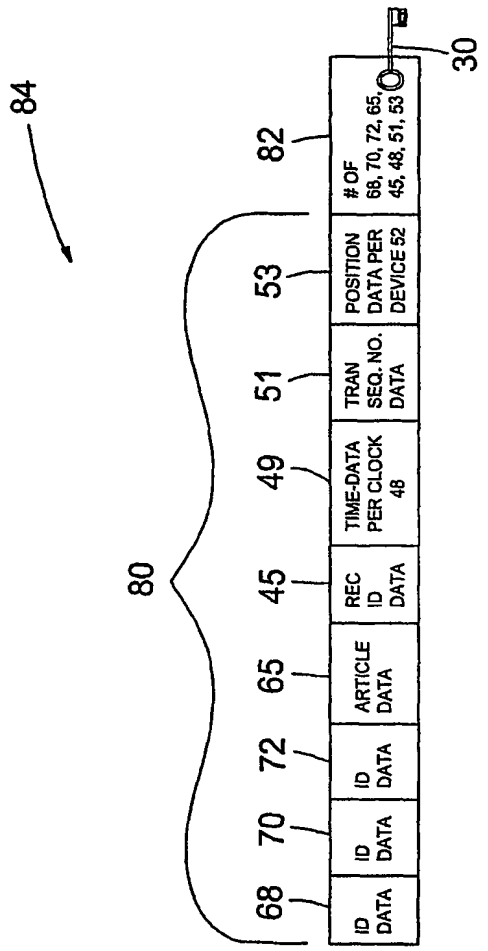
84
80
68
70
72
65
45
49
51
53
82
30
ID DATA
ID DATA
ID DATA
ARTICLE DATA
REC ID DATA
TIME-DATA PER CLOCK 48
TRAN SEQ. NO. DATA
POSITION DATA PER DEVICE 52
OF 68, 70, 72, 65, 45, 48, 51, 53

FIGURE 3

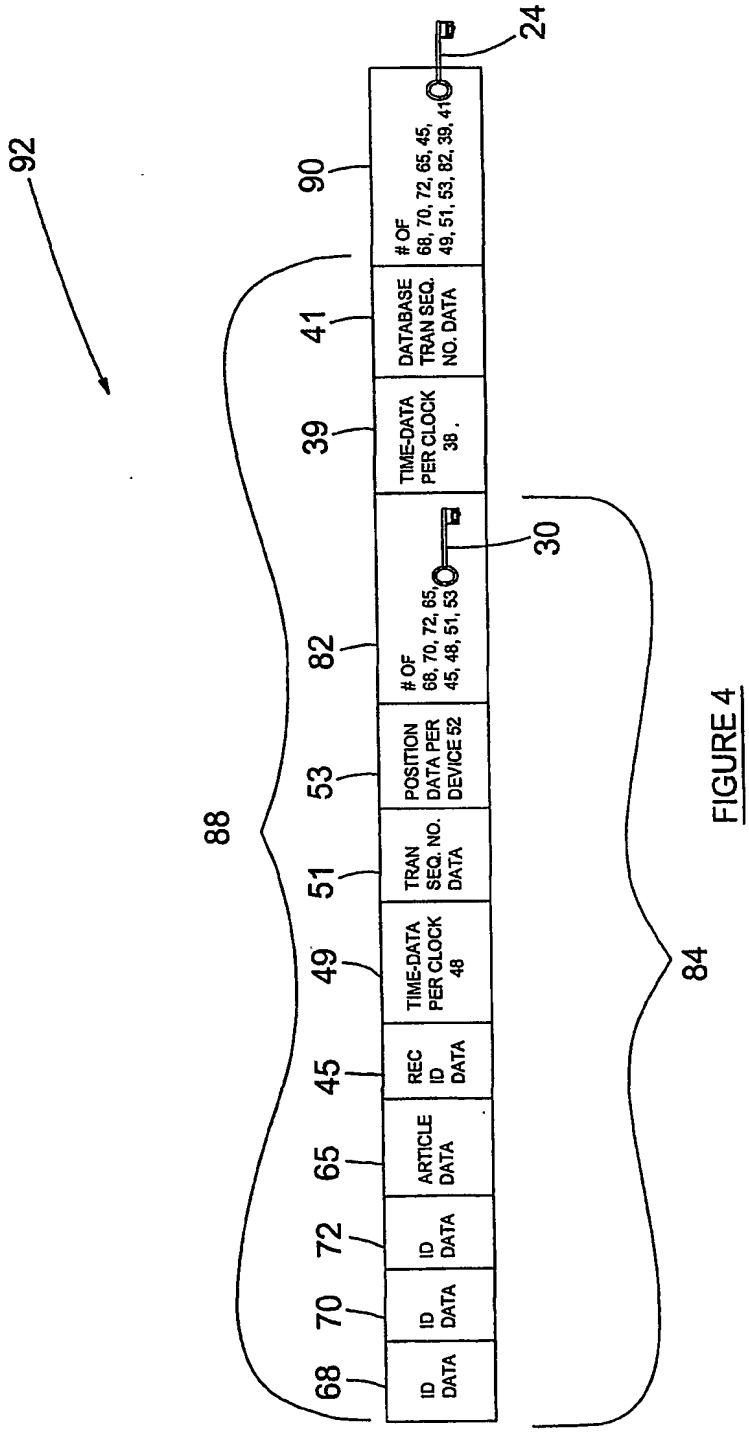
92
24
90
41
39
30
82
53
51
49
45
65
72
70
68
88
84
ID DATA
ID DATA
ID DATA
ARTICLE DATA
REC ID DATA
TIME-DATA PER CLOCK 48
TRAN SEQ. NO. DATA
POSITION DATA PER DEVICE 52
OF 68, 70, 72, 65, 45, 48, 51, 53
TIME-DATA PER CLOCK 38
DATABASE TRAN SEQ. NO. DATA
OF 68, 70, 72, 65, 45, 49, 51, 53, 82, 39, 41

FIGURE 4

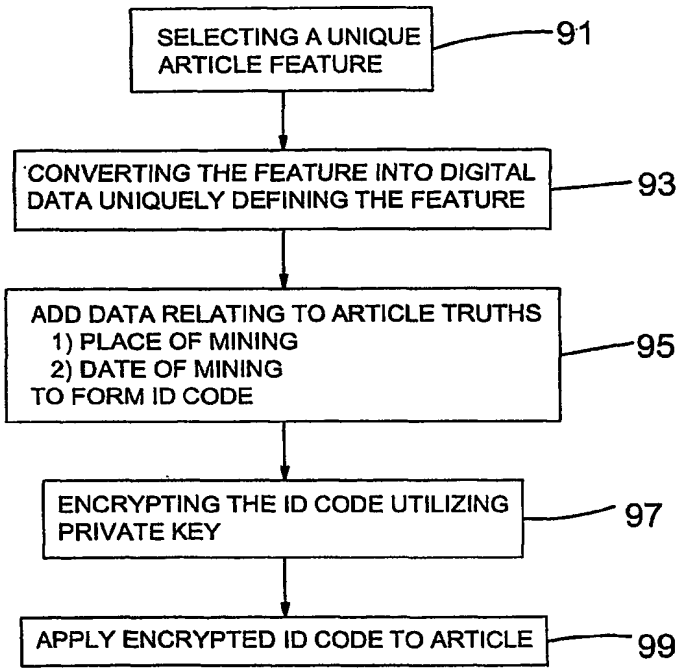
SELECTING A UNIQUE ARTICLE FEATURE
91
CONVERTING THE FEATURE INTO DIGITAL DATA UNIQUELY DEFINING THE FEATURE
93
ADD DATA RELATING TO ARTICLE TRUTHS
1) PLACE OF MINING
2) DATE OF MINING
TO FORM ID CODE
95
ENCRYPTING THE ID CODE UTILIZING PRIVATE KEY
97
APPLY ENCRYPTED ID CODE TO ARTICLE
99

FIGURE 5

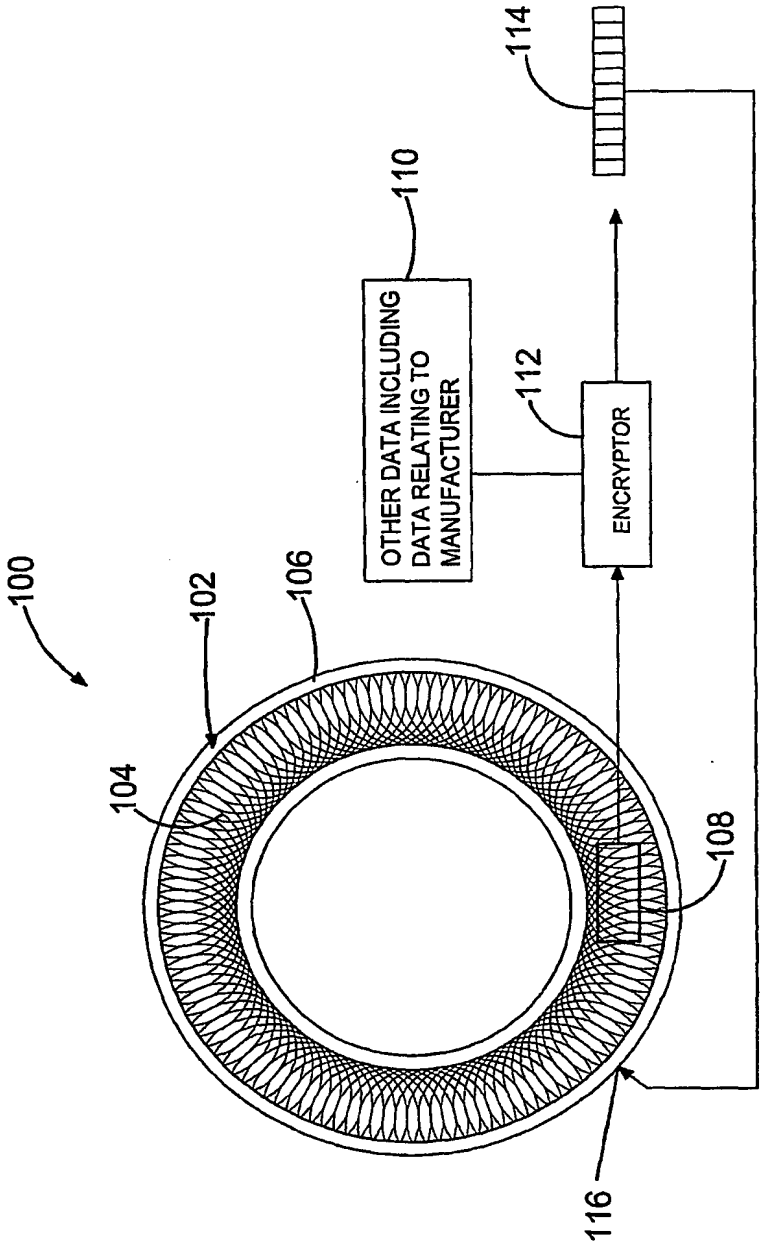
100
102
104
106
108
110
112
114
116
OTHER DATA INCLUDING DATA RELATING TO MANUFACTURER
ENCRYPTOR

FIGURE 6

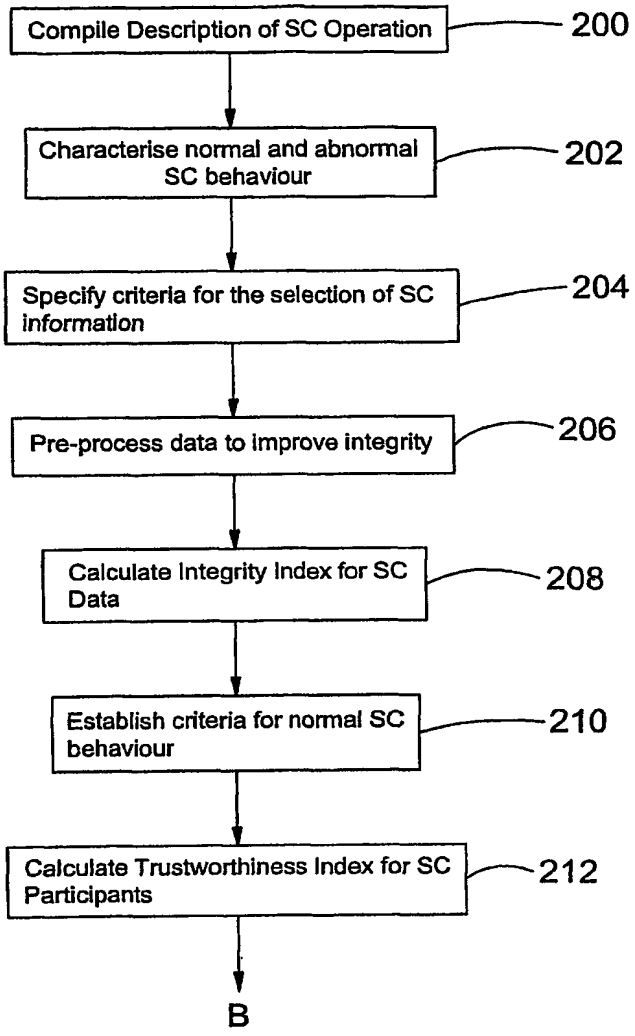
Compile Description of SC Operation
200
Characterise normal and abnormal SC behaviour
202
Specify criteria for the selection of SC information
204
Pre-process data to improve integrity
206
Calculate Integrity Index for SC Data
208
Establish criteria for normal SC behaviour
210
Calculate Trustworthiness Index for SC Participants
212
B

FIGURE 7(a)

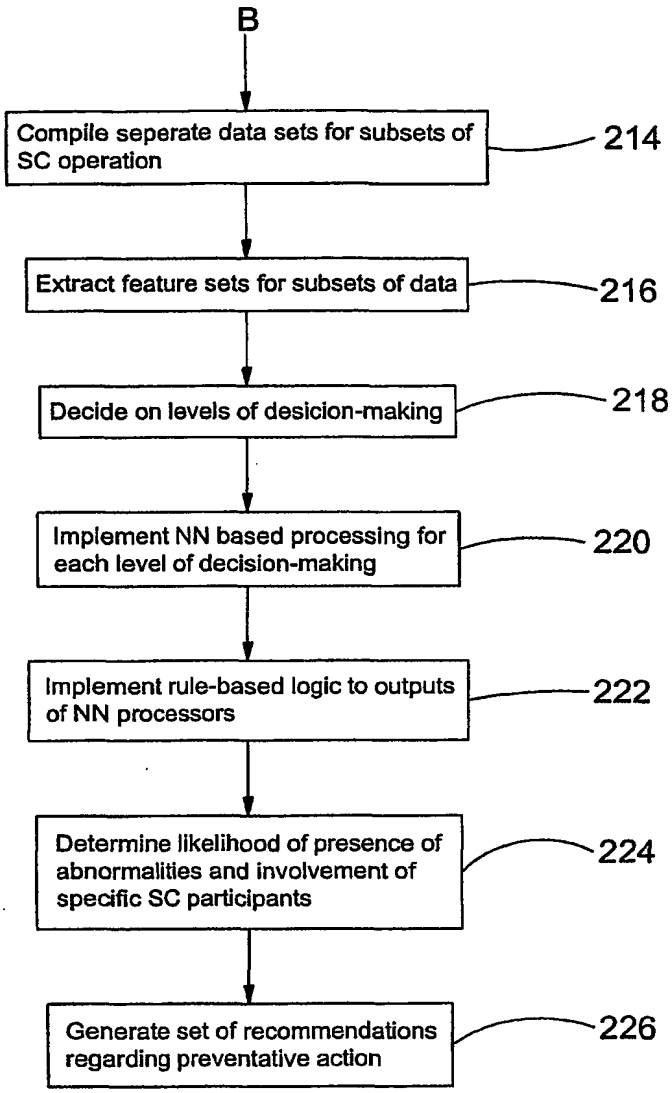
B
Compile seperate data sets for subsets of SC operation
214
Extract feature sets for subsets of data
216
Decide on levels of desicion-making
218
Implement NN based processing for each level of decision-making
220
Implement rule-based logic to outputs of NN processors
222
Determine likelihood of presence of abnormalities and involvement of specific SC participants
224
Generate set of recommendations regarding preventative action
226

FIGURE 7(b)

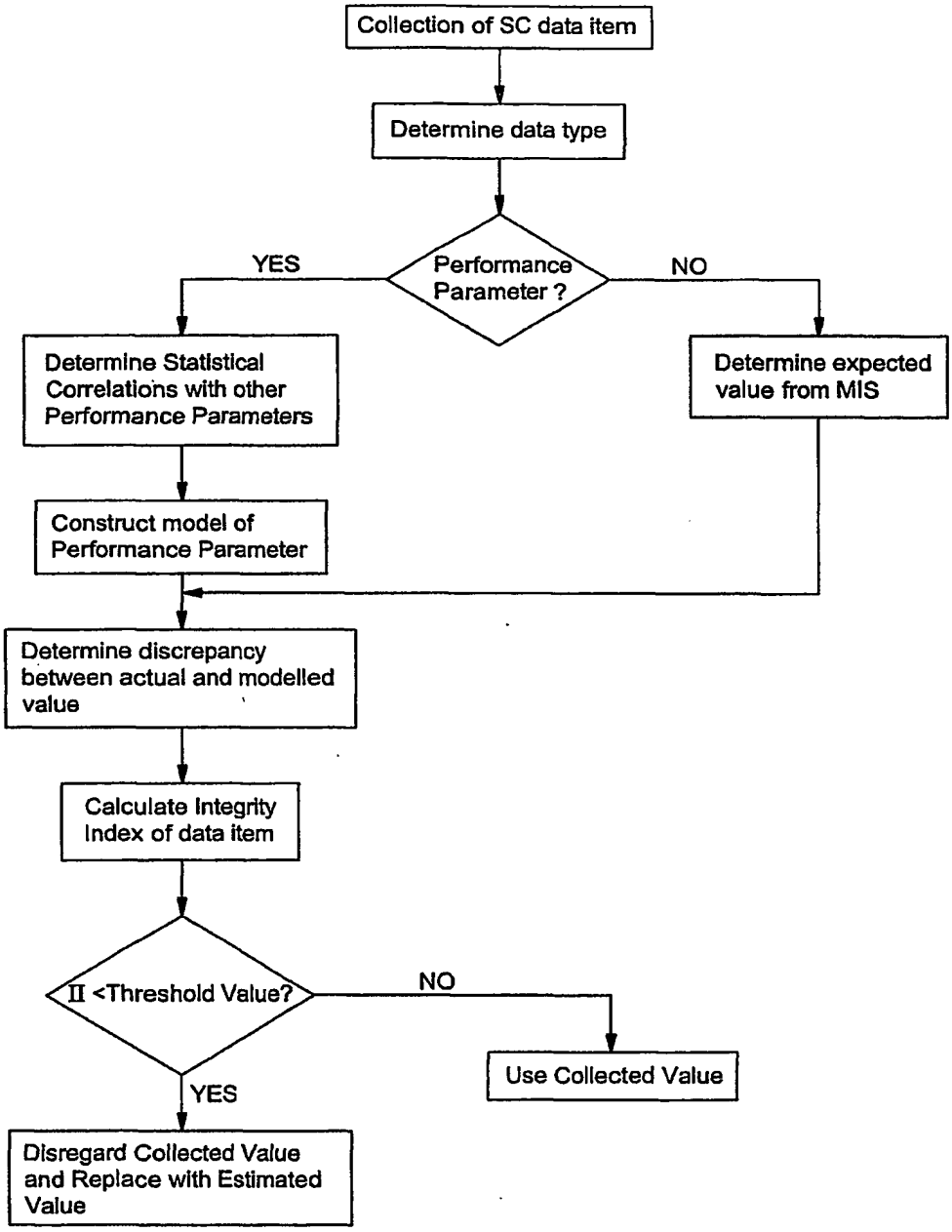
Collection of SC data item
Determine data type
Performance Parameter ?
YES
NO
Determine Statistical Correlations with other Performance Parameters
Determine expected value from MIS
Construct model of Performance Parameter
Determine discrepancy between actual and modelled value
Calculate Integrity Index of data item
II <Threshold Value?
NO
YES
Use Collected Value
Disregard Collected Value and Replace with Estimated Value

FIGURE 8

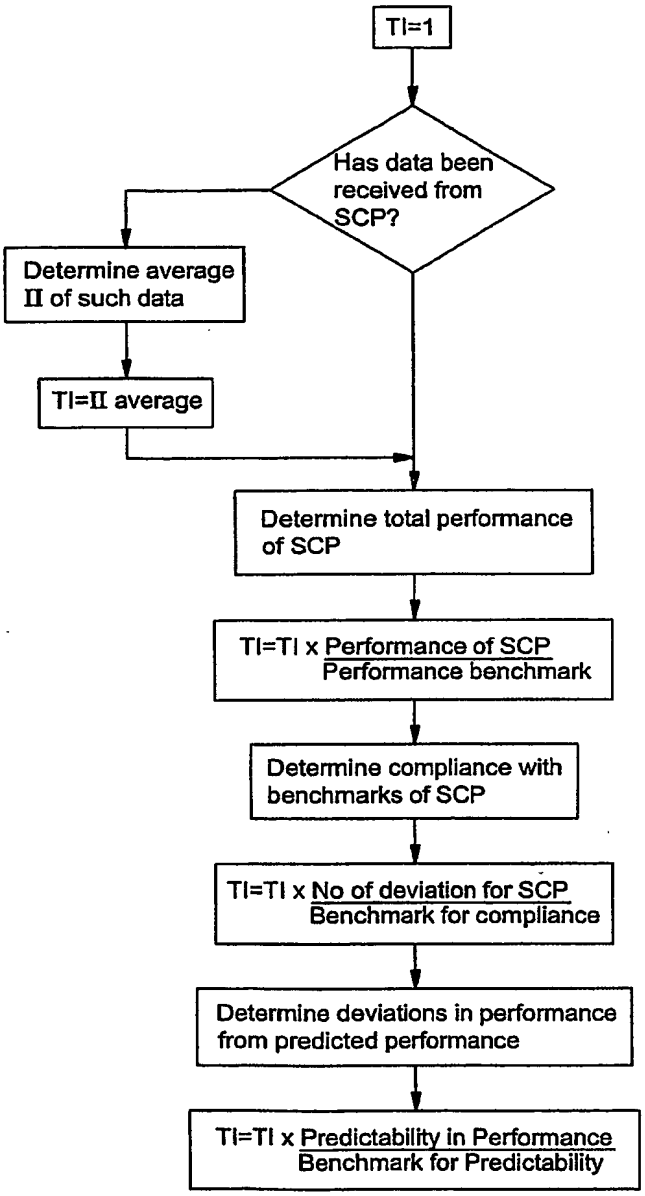
TI=1
Has data been received from SCP?
Determine average II of such data
TI=II average
Determine total performance of SCP
TI=TI x Performance of SCP / Performance benchmark
Determine compliance with benchmarks of SCP
TI=TI x No of deviation for SCP / Benchmark for compliance
Determine deviations in performance from predicted performance
TI=TI x Predictability in Performance / Benchmark for Predictability

FIGURE 9

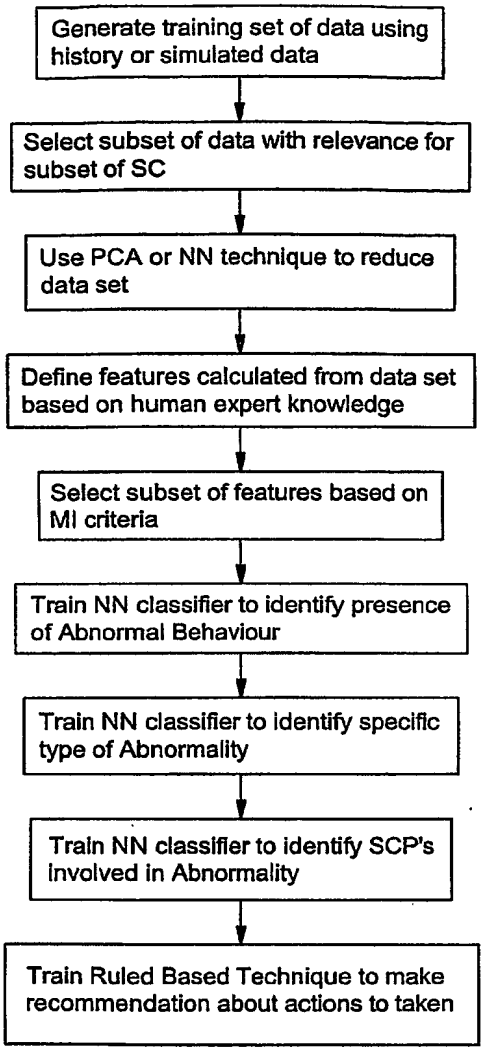
Generate training set of data using history or simulated data
Select subset of data with relevance for subset of SC
Use PCA or NN technique to reduce data set
Define features calculated from data set based on human expert knowledge
Select subset of features based on MI criteria
Train NN classifier to identify presence of Abnormal Behaviour
Train NN classifier to identify specific type of Abnormality
Train NN classifier to identify SCP's involved in Abnormality
Train Ruled Based Technique to make recommendation about actions to taken

FIGURE 10

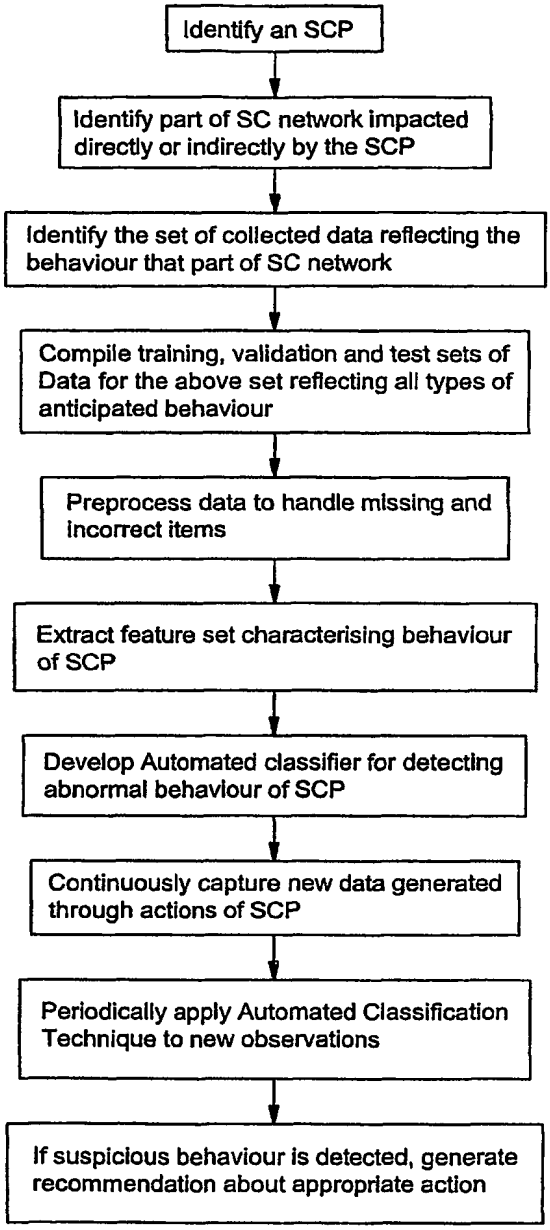
Identify an SCP
Identify part of SC network impacted directly or indirectly by the SCP
Identify the set of collected data reflecting the behaviour that part of SC network
Compile training, validation and test sets of Data for the above set reflecting all types of anticipated behaviour
Preprocess data to handle missing and incorrect items
Extract feature set characterising behaviour of SCP
Develop Automated classifier for detecting abnormal behaviour of SCP
Continuously capture new data generated through actions of SCP
Periodically apply Automated Classification Technique to new observations
If suspicious behaviour is detected, generate recommendation about appropriate action

FIGURE 11

	L_1	L_2	L_3	L_4	L_5	Result	
V_{A1}	2	1	1	1	1	in order	–128
t_{A1}	1	2	2	3	3		–130
V_{A2}	1	1	1	1	1	problem	–132
t_{A2}	1	2	4	3	5		–134
V_{A3}	1	-	1	-	1	in order	–136
t_{A3}	1	-	2	-	3		–138
V_{A4}	2	-	1	1	1	suspect but in order	–140
t_{A4}	1	2	2	3	3		–142

FIGURE 12